



**U.S. DEPARTMENT OF COMMERCE
MANUAL OF SECURITY
POLICIES AND PROCEDURES**

Chapter 10 - Position Designation

1001 Position Risk and Sensitivity Designation

All positions in the Department must be evaluated and assigned a sensitivity and/or a risk designation commensurate with the duties and responsibilities related to national security and/or to the efficiency of the service. The purpose of designating position sensitivity or risk level is to ensure that the incumbent undergoes the appropriate type of investigative processing and fulfills the requirements under Executive Order (E.O.) 10450, Security Requirements for Government Employment, and the Code of Federal Regulations, 5 CFR Parts 731 and 732.

A. Responsibility for Position Designation.

1. The head of each operating unit or departmental office, in consultation with their servicing human resources management office, shall ensure that each employee's position in the operating unit or office is designated at the appropriate level of position sensitivity and/or risk and that this designation is clearly stated in the employee's position description. The criterion for risk designation is contained in DAO 202-731, Handbook on Suitability. This Handbook delegates to heads of operating units and servicing human resources managers the authority to designate the sensitivity and risk level for each position in their operating units or departmental offices. Heads of operating units or departmental offices may delegate this authority to subordinate managers and supervisors who have been delegated personnel management authority. See paragraph 1002 below for a description of the designation of employee positions.
2. Positions established by contract in a departmental facility or other direct association by a non-employee shall be designated with a position sensitivity and/or a risk level. Criteria for designating contract positions are discussed in paragraph 1003 below. All contracts that involve access to classified information are processed through the Office of Security. For unclassified contract work, the responsibility for designating the risk level is shared by the contracting officer and operating unit management.

B. Basis for Position Designation.

1. The position sensitivity and risk level designation of a position must be based on an overall assessment of the damage that an individual, by virtue of occupying the position, could cause to national security or to the efficiency or integrity of departmental operations, also known as "the efficiency of the service."



**U.S. DEPARTMENT OF COMMERCE
MANUAL OF SECURITY
POLICIES AND PROCEDURES**

a. Sensitivity designations are given for national security positions and involve an assessment of the following considerations:

(1) Duties and responsibilities of a position that impact directly or indirectly on the interests of national security, including access to classified information under E.O. 12968 or similar authority, or access to sensitive, restricted facilities; or

(2) Automated Data Processing (ADP) security functions that relate to the potential risks involving national security.

b. Risk level designations are given to all positions and involve an assessment of the following considerations:

(1) Duties and responsibilities of a position that impact directly or indirectly on the Department's mission or on the efficiency of the service, including consideration of public safety, the protection of public property, and public trust; or

(2) Automatic Data Processing (ADP) functions that relate to the potential risks involving the mission of the Department.

2. Upon completion of the assessment of both sensitivity and risk, the higher designation level between the two assessments becomes the minimum risk or sensitivity designation for the position and dictates the level of investigation required for the incumbent in the position.

C. Coding of Position Designation Levels.

Servicing security officers shall maintain a record of the position designations levels for each national security sensitive position in the operating unit or office they support. The following position designation codes must be used when initiating an investigation into an individual's background. Paragraph 1002 defines these designations.

<u>Level</u>	<u>Coding</u>
Special-Sensitive (SS)	4
Special-Sensitive ADP	4C
Critical-Sensitive (CS)	3
Critical-Sensitive ADP	3C
Noncritical-Sensitive (NCS)	2



**U.S. DEPARTMENT OF COMMERCE
MANUAL OF SECURITY
POLICIES AND PROCEDURES**

Noncritical-Sensitive ADP	2C
High Risk (HR)	6
High Risk ADP	6C
Moderate Risk (MR)	5
Moderate Risk ADP	5C
Low Risk (LR)	1
Low Risk ADP	1C

1002 Designation of Employee Positions

All employee positions in the Department of Commerce require a risk designation. In addition, positions that require access to national security information must also have a sensitivity designation. The level of investigation required for a position is determined by its risk or sensitivity designation. The level of investigation required by the sensitivity designation will normally take precedence over that required by the risk designation. The exception to this requirement would be the investigation for a High Risk position requiring access to national security information at the Secret level. Guidance for the designation of sensitive positions is outlined below.

A. National security (sensitive) positions may be designated **Special-Sensitive, **Critical-Sensitive**, or **Noncritical-Sensitive**.**

1. **Special-Sensitive (SS)** positions include any position that the head of an operating unit determines to be designated at a level higher than Critical-Sensitive. This may be due to special requirements under an authority other than E.O. 10450 and E.O. 12968 (such as DCID 6/4 that sets investigative requirements and standards for access to Sensitive Compartmented Information (SCI) and other intelligence-related Special Sensitive information.

2. **Critical-Sensitive (CS)** positions have the potential for exceptionally grave damage to the national security. These positions may include access up to, and including, Top Secret defense information; development or approval of war plans, plans or particulars of future, major, or special operations of war, or critical and extremely important items of war; investigative duties, the issuance of personnel security clearances, or duty on personnel security boards; or other positions related to national security, regardless of duties, that require the same degree of trust.

3. **Noncritical-Sensitive (NCS)** positions have the potential for serious damage to the national security. These positions involve either access to Secret or Confidential national security information or materials or



U.S. DEPARTMENT OF COMMERCE MANUAL OF SECURITY POLICIES AND PROCEDURES

to duties that may adversely affect, directly or indirectly, the national security operations of the Department.

B. Non-national security (risk) positions may be designated **High Risk, **Moderate Risk**, or **Low Risk**.**

1. **High Risk (HR)** positions have the potential for exceptionally serious impact involving duties especially critical to the Department or a program mission with broad scope of policy or program authority. Examples include policy development and implementation, higher-level management assignments, independent spokespersons or non-management positions with authority for independent action, or significant fiduciary and procurement responsibilities.

2. **Moderate Risk (MR)** positions have the potential for moderate to serious impact involving duties of considerable importance to the Department or program mission with significant program responsibilities and delivery of customer services to the public. Examples include assistants to policy development and implementation, mid-level management assignments, non-management positions with authority for independent or semi-independent action, or delivery of service positions that demand public confidence or trust.

3. **Low Risk (LR)** positions involve duties that have a low or limited impact on the Department's mission or on the efficiency of the service.

C. Additional factors for determining the minimum position risk level.

1. **Uniqueness.** Factors unique to a particular position that are not accounted for elsewhere in the position designation process may cause adjustments to the position designation level. Examples include:

- a. Special investigative or law enforcement positions requiring possession and use of a firearm.
- b. Access to or control of highly sensitive but unclassified information.
- c. Access to sensitive financial records or control of an automated monetary system (e.g., key access entry);
- d. Few-of-a-kind positions with sensitive duties (e.g., special assistant to an agency head); or
- e. Support positions with no responsibilities for preparation or implementation of sensitive program



**U.S. DEPARTMENT OF COMMERCE
MANUAL OF SECURITY
POLICIES AND PROCEDURES**

policies and plans, but which involve regular contact with and on-going knowledge of all, or most of, such material (e.g., budget analyst).

2. **Uniformity.** Uniformity of position designations may be necessary because the authority level or program placement level may serve as a basis for the designation. Examples include:

a. An agency head may adjust position designations at the same authority level to assure uniformity within the agency (e.g., managers of major agency programs at the same level of authority may be placed at the same level of risk), or

b. An agency head may place all positions within a program at the same position designation level if the risk to the program is such that, although no specific risks are associated with the position, the position involves work in an environment that can create a general risk to the program.

3. **Public Trust Positions.** Positions at the High or Moderate Risk levels are designated as “Public Trust” positions. Such positions may involve policy making, major program responsibility, public safety and health, law enforcement duties, fiduciary responsibilities, or other duties demanding a significant degree of public trust; and positions involving access to or operation or control of financial records, with a significant risk for causing damage or realizing personal gain.

1003 Designation of Non-Employee Positions

A. Position Designation for Non-Classified Contracts. The Contracting Officer’s Technical Representative (COTR), in conjunction with operating unit management, servicing security officer, and security contact, will review the work to be performed under contract and assign the highest risk designation to the entire contract in accordance with the criteria stated below. Accordingly, each contract employee will undergo investigative processing based on the contract’s risk level designation (see paragraph 1104).

1. **High Risk.** A contract will be designated High Risk if it meets the following criteria:

a. Work requiring continuous foreign travel of 90 days or more at any time during the performance of the contract under the auspices of the Department;

b. Work involving functions or operations of the Department that are critical to the accomplishment of the mission of the Department;



U.S. DEPARTMENT OF COMMERCE MANUAL OF SECURITY POLICIES AND PROCEDURES

- c. Work involving investigative, compliance, or senior-level auditing duties;
- d. Work involving fiduciary, public contact, or other duties involving the highest degree of public trust;
- e. Work involving Automatic Data Processing functions such as:
 - (1) Planning, directing, and implementing a computer security program;
 - (2) Planning, designing, directing, and operating a computer system that includes ADP hardware, software, and/or data communications, regardless of the sensitivity or classification of the information stored on the system; or
 - (3) Access to a computer system, during the operation or maintenance process that could result in grave damage or in personal gain; or
- f. Any other work designated High Risk by the contracting officer or by the head of the operating unit or departmental office.

2. **Moderate Risk.** A contract will be designated Moderate Risk if it meets the following criteria:

- a. Work involving free access and movement during normal work hours within a Department of Commerce facility which houses classified information or equipment with little or no supervision by an appropriately cleared Federal Government employee;
- b. Work occurring during restricted hours within a Department of Commerce facility which houses classified or sensitive information or equipment even though supervised by a Federal Government employee;
- c. Work in which a contractor is responsible for the direction, planning, design, operation, or maintenance of a computer system, and whose work is technically reviewed by Federal Government personnel whose position sensitivity is Critical-Sensitive or above to ensure the integrity of the system;
- d. Work requiring access to sensitive information (information protected under the Privacy Act or Title 13 of the U.S. Code); or
- e. Work involving foreign travel less than 90 days duration.



U.S. DEPARTMENT OF COMMERCE MANUAL OF SECURITY POLICIES AND PROCEDURES

3. **Low Risk.** Work that does not fall into any of the categories noted above will be given a Low Risk designation.

B. Variance in Contract Responsibilities. In instances where there is a wide variance in the risk level of the work to be performed under one contract, individual contract employees may be processed at a lower risk designation based on their duties when approved by the servicing security officer. However, the contract document must specifically apply controls to ensure that the work of persons in the lower risk positions will not overlap with that for the higher risk positions. The contract will identify the number of employees to be processed at the lower risk designation and will specify the duties of the positions. An example of such a case is custodial work where some contract employees perform work that is not supervised during security hours in a building which houses classified information, while others may work under close government supervision during normal work hours. The entire contract might be designated High or Moderate Risk due to the former case, but those contract employees whose work would be Low Risk would be processed with the appropriate background investigation. The contract must meet control obligations to ensure that there is no overlap of work duties between the two groups.

C. Position Designations for Classified Contracts. Classified contracts are handled under the auspices of the Department of Defense National Industrial Security Program (NISP). Generally, contract employees requiring access to national security information are not processed through the Department's Personnel Security Program. For guidance on classified contracts, refer to Chapter 43, Industrial Security, of this manual.

D. Position Designations for Other Non-employee Positions.

1. Experts and consultants are subject to the same security requirements as regular employees of the Department. Since experts and consultants are paid at a level equivalent to a GS-13 or above, such positions should be evaluated based on Public Trust criteria. If a position is not sensitive, experts and consultants should be evaluated as an employee would be for a High or Moderate Risk position.

2. Guest workers, research associates, trainees, long-term visitors, and other similar types of non-employees associated with the Department usually serve in a Low Risk capacity. There are no specific criteria for evaluating their involvement under risk designation criteria; however, the determination should take into account the potential impact or damage that the non-employee's interaction could cause. If the involvement of these non-employees falls within the generic description of a sensitive position, the manager of the operating unit involved must advise the Office of Security in accordance with this chapter of the Security Manual.



**U.S. DEPARTMENT OF COMMERCE
MANUAL OF SECURITY
POLICIES AND PROCEDURES**
